

# Message from the Program Manager, Information Sharing Environment

In the five years since the Congress directed the creation of the Information Sharing Environment (ISE), significant steps have been taken towards establishing a strong foundation. Important mission initiatives, such as Suspicious Activity Reporting and ISE core capabilities and enablers, such as fusion centers and the National Information Exchange Model, have produced results and show ongoing promise. The leaders and visionaries that drive these efforts are the mission owners and the frontline personnel—and they did this work while fighting an ever-evolving enemy.

The ISE is realized by the investment of mission partners—the bureaus and agencies of federal, state, and local, and tribal governments and our partners in the private sector and internationally—and made relevant through use by frontline law enforcement, public safety, homeland security, intelligence, defense, and diplomatic personnel. Ultimately, the ISE is neither more nor less than the contributions of the mission partners—they are the engines that build and operate the ISE. This report reflects their accomplishments and the efforts of the terrorism and homeland security [1](#) information sharing and access community. It broadly inventories initiatives that, taken together, should be seen as the foundational steps of building the ISE. Information sharing and access capabilities have improved over the past year. Yet, the persistent and evolving threat of terrorism compels us to accelerate delivery of results from a more clearly defined and mission-integrated ISE.

The purpose of the ISE is to exploit the existing strengths within our federated democracy and open society: to innovate and deploy new approaches and tools to effectively share, discover, fuse, and enable timely action on terrorism-related information while protecting our privacy and civil liberties. The scope of the ISE is across federal agencies; spanning all levels of government; between the public and private sectors; and with our international partners to enhance national security and protect the American people from terrorism. The primary focus of the ISE is any mission process, anywhere, which has a material impact on detecting, preventing, disrupting, responding to, or mitigating terrorist activity. The scope of the ISE is best described in terms of end-to-end counterterrorism and homeland security mission processes—such as watchlisting, screening, and suspicious activity reporting—along with supporting core capabilities and enablers.

Mission partners rarely have the ability to segregate their activities to isolate terrorism information. Frontline law enforcement agencies, for example, are more likely to generate suspicious activity reports relating to gang or narcotic crime than crime with a terrorism nexus. Flexibility in the Nationwide Suspicious Activity Reporting Initiative is allowing local, state, tribal, and federal mission partners to capitalize on consistent training, privacy and civil liberty protections, oversight, and change management investments to consider moves toward information-led policing. Such mission partner equities must be considered to avoid deadlock or partial and ineffective solutions. The Program Manager for the ISE (PM-ISE) co-chairs the White House-based Information Sharing and Access Interagency Policy Committee, a forum that balances the ISE's core focus on terrorism and homeland security with ISE mission partners' needs to address the whole of national security-related information sharing and access challenges.

Key to progress in building the ISE, has been a relentless focus on identifying, integrating, and sharing

best practices. Broad adoption of best practices raises confidence, lowers risk, and accelerates adoption, use, and reuse resulting in a strong return on investment by mission partners. In particular, the adoption of best practices has utility beyond the terrorism information sharing mission, extending both across complementary missions and into new mission areas unrelated to terrorism. With the ISE, smart management and good policy come together.

The support of mission partners is critical to the success of the ISE. They have mission responsibility and a vital leadership role for delivery, operation, and use of the ISE, and are accountable for delivering value by aligning policy, processes, and information. The role of PM-ISE is to bring ISE mission partners together to collaborate and support shared, cross-organizational solutions based on collective mission equities, to build consensus to prioritize funding and deliver on the shared vision, and to provide a collective management and governance framework to accelerate nationwide results. This is a team effort that requires maintaining engagement and persuading stakeholders to accept the wisdom and value of contributing to the build-out and use of the ISE, while addressing perceptions of risk and lack of control.

Going forward, we will continue working with mission partners and expand our aperture to address end-to-end terrorism-related mission processes across all levels of government, while tightening our focus on the technology-enabled, mission partner-based, network-centric vision of the ISE described in the Intelligence Reform and Terrorism Prevention Act of 2004. Over the next year, the following steps will build on, reinforce, and help accelerate the initiatives profiled in this report:

- Strengthen governance, engagement, and alignment across ISE stakeholders;
- Refresh the National Strategy for Information Sharing;
- Build capacity through increased emphasis on agency-based centers of excellence;
- Promote a culture of continuous improvement and innovation; and
- Clarify and deepen relationships with other government-wide organizations and leaders

Several events this past year—the Zazi case, the Fort Hood Shooting and the attempted bombings on Christmas Day and in Times Square—highlight challenges, successes, and gaps in our ability to effectively share and access information. Looking back to the events of September 11, 2001, we have come far in our sharing of and access to information across boundaries organizational boundaries and mission domains. Yet much remains to be done to support the frontline. Whether they are countering violent extremists overseas, protecting our borders and waterways, or patrolling the streets of American cities, the brave men and women of the frontline that fight terrorism and protect our homeland need timely, accurate, and relevant information to do their jobs effectively. We have work to do.

<sup>1</sup> Section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), P.L. 108-485, § 1016, 118 Stat. 3638, 3664 (2004), as amended, directs the ISE to improve the sharing of Terrorism and Homeland Security Information. The IRTPA definition of Terrorism Information encompasses all terrorism-related information “whether collected, produced, or distributed by intelligence, law enforcement, military, homeland security, or other activities,” and was explicitly amended in 2007 to include Weapons of Mass Destruction Information. For brevity, these types of information are collectively referred to as “terrorism-related” information.